**CORE SERVICE DESIGN:**

**Storage Account and Blob**

atabricks

|  |  |
| --- | --- |
| IT Owner Details | |
| **Department** | DTS |
| **Contact Name** | Dominic Panzera |
| **Address** | 375 Manningham Road, Doncaster, Victoria 3108 |

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Storage Account and Blob Core Service Design |
| **File Name** | Ambulance Victoria – Storage Account and Blob Core Service Design v1.0.docx |
| **Version** | 1.0 |
| **Status** | Released |
| **Release Date** | 18/01/2024 |

|  |  |  |  |
| --- | --- | --- | --- |
| Preparation |  |  |  |
| **Prepared** | Daniela Nikolic |  |  |
| **Authorised** | Dileep Pradeep |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| **Version** | **Remarks** | **Change Requested** | **Pages Affected** | **Release Date** |
| 1.0 | Initial Release | N/A | All | 18/01/2024 |

Table of Contents

[1. Overview 5](#_Toc156400005)

[1.1 Purpose and Audience 5](#_Toc156400006)

[1.2 Scope and Key Deliverables 5](#_Toc156400007)

[1.3 Glossary and Definitions 6](#_Toc156400008)

[2. Executive Summary 7](#_Toc156400009)

[3. Resource Cost 7](#_Toc156400010)

[4. WAF and Security Control Alignment 8](#_Toc156400011)

[4.1 Reliability 8](#_Toc156400012)

[4.1.1 Overview 8](#_Toc156400013)

[4.1.2 Storage Account and Blob Reliability Checklist 8](#_Toc156400014)

[4.2 Cost Optimisation 10](#_Toc156400015)

[4.2.1 Overview 10](#_Toc156400016)

[4.2.2 Storage Account and Blob Cost Optimisation Checklist 10](#_Toc156400017)

[4.3 Operational Excellence 11](#_Toc156400018)

[4.3.1 Overview 11](#_Toc156400019)

[4.3.2 Storage Account and Blob Operational Excellence Checklist 11](#_Toc156400020)

[4.4 Performance Efficiency 11](#_Toc156400021)

[4.4.1 Overview 11](#_Toc156400022)

[4.4.2 Storage Account and Blob Performance Efficiency Checklist 11](#_Toc156400023)

[4.5 Security 12](#_Toc156400024)

[4.5.1 Overview 12](#_Toc156400025)

[5. Architecture Summary 13](#_Toc156400026)

[5.1 Resource Overview 13](#_Toc156400027)

[5.2 RBAC 14](#_Toc156400028)

[5.3 Design Decisions and Justifications 15](#_Toc156400029)

[5.3.1 Storage Account Type Selection 15](#_Toc156400030)

[5.3.2 Blob Tier Selection 15](#_Toc156400031)

[5.3.3 Redundancy 15](#_Toc156400032)

[5.3.4 Soft Delete 16](#_Toc156400033)

[5.3.5 Access and Authentication 16](#_Toc156400034)

[5.3.6 Managed Identities 16](#_Toc156400035)

[5.3.7 Blob Versioning and Immutability 17](#_Toc156400036)

[5.3.8 Network Access 17](#_Toc156400037)

[5.3.9 Secure Transfer 17](#_Toc156400038)

[5.3.10 Shared Access Keys 18](#_Toc156400039)

[5.3.11 SAS (Shared Access Signatures) 18](#_Toc156400040)

[5.3.12 Blob Lifecycle Management 18](#_Toc156400041)

[5.3.13 Data Protection 19](#_Toc156400042)

[5.3.14 Defender for Storage 19](#_Toc156400043)

[5.3.15 Data Encryption at Rest and In Transit 19](#_Toc156400044)

[5.3.16 Logging and Monitoring 20](#_Toc156400045)

[5.3.17 Backup 20](#_Toc156400046)

[6. Azure Policies 20](#_Toc156400047)

[7. Configuration Templates 21](#_Toc156400048)

[7.1 Platinum Production 21](#_Toc156400049)

[7.2 Platinum DR 22](#_Toc156400050)

[7.3 Gold and Silver 23](#_Toc156400051)

[7.4 Bronze Non-Production 24](#_Toc156400052)

[8. Acceptance 25](#_Toc156400053)

# Overview

This document covers the baseline design for the Storage Account and Blob core service. The intention of this document is to define the overall resource design in isolation from a specific application. It is aimed to highlight the general process and requirements for building a Storage Account and Blob in a repeatable fashion with consistent configurations. Design decisions and justifications have been included in the Architecture section, and this document can be used as a reference for new builds that require a Storage Account and Blob.

This design caters to a Level 2 design which covers both Microsoft’s WAF (Well Architected Framework)[[1]](#footnote-2) and the Department of Health Control list.

Any deviations required to the standards defined in this document will require separate exemption and approval from the Cloud Governance Forum if they are required for any reason for a specific build.

## Purpose and Audience

This document will outline the standard design and configuration of this Azure service in Ambulance Victoria’s Azure tenancy as a baseline for any application infrastructure deployments.

This design is intended to:

* Meet Microsoft WAF standards.
* Meet the controls stipulated by the Department of Health.
* Define the baseline required for the deployment of the resource.

The audience for this document is those involved in the planning, designing, and implementing of the Application/Data infrastructure. This includes:

* + Ambulance Victoria IT staff

It is assumed that the reader knows and is familiar with Azure Cloud concepts and related topics.

## Scope and Key Deliverables

The scope of this core service design is to define the baseline deployment requirements and standards for the Storage Account and Blob core service.

The key deliverables for this are:

* This design to outline the service definition Level 2 baseline standards.
* A technical configuration document that defines the deployment of this resource for each of the Service Tiers, or for any other logical standard such as size
* IaC templates for repeatable deployment of this core service

## Glossary and Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **AV** | Ambulance Victoria |
| **WAF** | Well Architected Framework |
| **CAF** | Cloud Adoption Framework |
| **Level 1** | Refers to a resource that has been designed to a CAF standard |
| **Level 2** | Refers to a resource that has been designed to a WAF standard with Department of Health controls overlayed |
| **AZ 2** | Refers to Ambulance Victoria’s legacy Azure Landing Zone still in use in some regards |
| **AZ 3** | Refers to Ambulance Victoria’s current Azure Landing Zone, also referred to as the Enterprise landing zone. This is the target state for migrations. |
| **SLA** | Service Level Agreement as defined by Microsoft |
| **SA** | Storage Account |
| **DH** | Department of Health |
| **IaC** | Infrastructure as Code |
| **NSG** | Network Security Groups |
| **GRS** | Geo-Redundant Storage |
| **LRS** | Locally-Redundant Storage |
| **RA-GRS** | Read Access Geo-Redundant Storage |

Table : Glossary and definitions

# Executive Summary

This design covers the baseline standards for the Storage Account and Blob Core Service. This service has been assessed against the five pillars of WAF as well as the Department of Health Security Controls.

This section contains a summary of the major design decisions that have been made for defining the baseline of this resource as an outcome of the WAF and Security analysis detailed throughout this document.

Of the five WAF Pillars, it was found that Reliability, Cost Optimistaion, and Security were applicable. The guidance for Operational Excellence was identical to Reliability so it has not been repeated. The majority of the Security guidance also overlapped with Reliability, so it has not been repeated.

For this service the main baseline configurations include:

* General Purpose v2 will be the default account type. Other types should only be used by exception.
* All service tiers will have Minimum TLS of 1.2
* All service tiers will use Azure AD (Entra ID) authentication with access keys disabled by default.
* The same Lifecycle Management policies will be implemented on all tiers
* Private networking will be used.
* All deployments will use the Hot tier as the default.

There are some notable differences across the service tier configurations for this service:

* The retention and backup policies will generally be:
  + 30 days for Platinum
  + 14 days for Gold and Silver
  + 7 days for Bronze
* Locally-Redundant storage will be used for Bronze tier deployments, and Read Access Geo-Redundant Storage will be used for Platinum, Silver, and Gold.

# Resource Cost

The cost of Azure Storage varies greatly depending on the settings chosen and the sub-services utilised[[2]](#footnote-3). As discussed in the Design Decisions section, the most recommended type of Storage Account is a General Purpose v2. The pricing calculator should be used to determine estimated costs prior to deployment when more information is on hand.

# WAF and Security Control Alignment

The following are the five pillars of the Microsoft Well Architected Framework:

* [Reliability](https://learn.microsoft.com/en-us/azure/well-architected/#reliability)
* [Cost optimization](https://learn.microsoft.com/en-us/azure/well-architected/#cost-optimization)
* [Operational excellence](https://learn.microsoft.com/en-us/azure/well-architected/#operational-excellence)
* [Performance efficiency](https://learn.microsoft.com/en-us/azure/well-architected/#performance-efficiency)
* [Security](https://learn.microsoft.com/en-us/azure/well-architected/#security)

For this design, the security section will also cover the Department of Health Controls in addition with any Microsoft Security Best Practices. Each of these sections will detail relevant controls or baseline requirements for this core service that will be put in place.

## Reliability

### Overview

The term reliability refers to the availability of the system and its ability to recover from failure[[3]](#footnote-4). Resiliency strategies must be built into each element of the architecture. The pillars of reliability include:

* Design for business requirements
* Design for failure
* Observe application health
* Drive Automation

### Storage Account and Blob Reliability Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Design | Enforcement Option | Applicability |
| **R1** | Turn on soft delete for blob data. | Yes | Yes | IaC | At deployment |
| **R2** | Use Microsoft Entra ID to authorize access to blob data. | Yes | Yes | IaC | At deployment |
| **R3** | Consider the principle of least privilege when you assign permissions to a Microsoft Entra security principal through Azure RBAC. | Yes | No | Governance | Operational |
| **R4** | Use managed identities to access blob and queue data. | Yes | No | Governance | Operational – at deployment of other applications |
| **R5** | Use blob versioning or immutable blobs to store business-critical data. | Yes | Yes | IaC | At deployment |
| **R6** | Restrict default internet access for storage accounts. | Yes | Yes | IaC | At deployment |
| **R7** | Enable firewall rules. | Yes | Yes | IaC | At deployment |
| **R8** | Limit network access to specific networks. | Yes | Yes | IaC | At deployment |
| **R9** | Allow trusted Microsoft services to access the storage account. | Yes | Yes | IaC | At deployment |
| **R10** | Enable the Secure transfer required option on all your storage accounts. | Yes | Yes | IaC | At deployment |
| **R11** | Limit shared access signature (SAS) tokens to HTTPS connections only. | Yes | Yes | IaC | At deployment |
| **R12** | Avoid and prevent using Shared Key authorization to access storage accounts. | Yes | Yes | IaC | At deployment |
| **R13** | Regenerate your account keys periodically. | Yes | Yes | Automation Account | At deployment |
| **R14** | Create a revocation plan and have it in place for any SAS that you issue to clients. | Yes | No | Governance | Operational – per SAS generated |
| **R15** | Use near-term expiration times on an impromptu SAS, service SAS, or account SAS. | Yes | No | Governance | Operational |

Table : WAF Reliability checklist summary

## Cost Optimisation

### Overview

The cost optimisation pillar is structured to support creating cost-effective workloads in the cloud[[4]](#footnote-5). It looks at removal of unnecessary spend and improving operational efficiency. The principles of cost optimisation revolve around:

* Choosing the correct resources
* Setting up budgets and maintaining cost constraints
* Dynamically allocate and deallocate resources
* Optimising workloads whilst aiming for scalable costs
* Continuously monitoring and cost managing

### Storage Account and Blob Cost Optimisation Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **CO1** | Periodically dispose and clean up unused storage resources, such as unattached disks and old snapshots. | Yes | No | Governance | Operational – review monthly |
| **CO2** | Consider Azure Blob access time tracking and access time-based lifecycle management. | Yes | Yes | IaC | At deployment |
| **CO3** | Transition your data from a hotter access tier to a cooler access tier if there's no access for a period | Yes | Yes | IaC | At deployment |
| **CO4** | Consider cost savings by reserving data capacity for block blob storage. | Yes | No | Governance | Operational – review annually |
| **CO5** | Organize data into access tiers. | Yes | No | Governance | Operational – at deployment of data |
| **CO6** | Use lifecycle policy to move data between access tiers. | Yes | Yes | IaC | At deployment |

Table : WAF Cost Optimisation checklist summary

## Operational Excellence

### Overview

Operational Excellence aims to ensure that once the architecture is built, the ongoing operations are flawless. This includes repeatable and reliable deployments, automating to eliminate human error. To do this the following must be considered:

* Optimise the build and release process (including CI/CD and IaC)
* Understand Operational Health
* Test recovery and failure
* Focus on continuous improvement
* Use loosely coupled architecture

### Storage Account and Blob Operational Excellence Checklist

The guidance for Operational Excellence for Azure Storage Accounts is identical to the guidance for Reliability so this information has not been repeated here.

## Performance Efficiency

### Overview

Performance Efficiency refers to the ability of your systems and applications to meet user demands without breaking or creating a negative user experience[[5]](#footnote-6). This covers capacity and scalability:

* Design for horizontal scaling
* Run stress and performance tests
* Continuously monitor performances, particularly in Production systems

### Storage Account and Blob Performance Efficiency Checklist

There is no guidance for Azure Storage Accounts under Performance Efficiency.

## Security

### Overview

Security refers to the ability of the environment to resist and manage threats.

This section covers both Microsoft Best Practices as well as relevant security controls provided by the Department of Health. With respect to the Microsoft WAF, Security is underpinned by the following[[6]](#footnote-7):

* Plan resources and how to harden them
* Automate and use least privilege
* Classify and encrypt data
* Monitor system security, plan incident response
* Identify and protect endpoints
* Protect against code-level vulnerabilities
* Model and test against potential threats

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark controls are applicable:

* NS-2: Secure cloud services with network controls
* IM-1: Use centralized identity and authentication system
* IM-3: Manage application identities securely and automatically
* IM-8: Restrict the exposure of credential and secrets
* DP-1: Discover, classify, and label sensitive data
* DP-2: Monitor anomalies and threats targeting sensitive data
* DP-3: Encrypt sensitive data in transit
* DP-4: Enable data at rest encryption by default
* DP-6: Use a secure key management process
* LT-4: Enable logging for security investigation
* BR-1: Ensure regular automated backups

# Architecture Summary

## Resource Overview

Azure Storage Account is the primary storage service in Azure. Within a Storage Account several sub-services can be utilised[[7]](#footnote-8):

* Blob
* File
* Queue
* Table

Storage Accounts in Azure are globally unique and can be accessed via HTTP or HTTPS.

There are several types of Storage Accounts that can be implemented summarised below:

|  |  |  |  |
| --- | --- | --- | --- |
| Type of storage account | Supported storage services | Redundancy options | Usage |
| Standard general-purpose v2 | Blob Storage (including Data Lake Storage)  Queue Storage  Table Storage  Azure Files | Locally redundant storage (LRS) / Geo-redundant storage (GRS) / read-access geo-redundant storage (RA-GRS)  Zone-redundant storage (ZRS) / geo-zone-redundant storage (GZRS) / read-access geo-zone-redundant storage (RA-GZRS)2 | Standard storage account type for blobs, file shares, queues, and tables. Recommended for most scenarios using Azure Storage. If you want support for network file system (NFS) in Azure Files, use the premium file shares account type. |
| Premium block blobs | Blob Storage (including Data Lake Storage1) | LRS  ZRS2 | Premium storage account type for block blobs and append blobs. Recommended for scenarios with high transaction rates or that use smaller objects or require consistently low storage latency. |
| Premium file shares | Azure Files | LRS  ZRS2 | Premium storage account type for file shares only. Recommended for enterprise or high-performance scale applications. Use this account type if you want a storage account that supports both Server Message Block (SMB) and NFS file shares. |
| Premium page blobs | Page blobs only | LRS  ZRS | Premium storage account type for page blobs only. |

Table : Summary of Storage Account Types

## RBAC

The following RBAC roles can be applied at the Storage Account level:

|  |  |
| --- | --- |
| Role Name | Description |
| Storage Account Backup Contributor | Lets you perform backup and restore operations using Azure Backup on the storage account. |
| Storage Account Contributor | Lets you manage storage accounts, including accessing storage account keys which provide full access to storage account data. |
| Storage Account Key Operator Service Role | Storage Account Key Operators are allowed to list and regenerate keys on Storage Accounts |

Table : RBAC roles relevant for the Storage Account

|  |  |
| --- | --- |
| Role Name | Description |
| Storage Blob Data Contributor | Allows for read, write and delete access to Azure Storage blob containers and data |
| Storage Blob Data Owner | Allows for full access to Azure Storage blob containers and data, including assigning POSIX access control. |
| Storage Blob Data Reader | Allows for read access to Azure Storage blob containers and data |
| Storage Blob Delegator | Allows for generation of a user delegation key which can be used to sign SAS tokens |

Table : RBAC roles relevant for the Blob Service

## Design Decisions and Justifications

This section covers the design decisions and justifications that reflect the findings of the WAF and Security alignment. This will form the baseline requirements for the Storage Account and Blob core service and will be captured in the accompanying Configuration Template with a set of pre-approved deployment settings for this resource. Any changes, modifications or removals to the pre-approved deployments must have specific approval from the Cloud Governance Forum prior to deployment.

### Storage Account Type Selection

**Design Reference:** N/A

**Design Decision**: General Purpose v2 will be set as the default option for Storage Account type. Other types can be used by exception if specifically required for an implementation.

**Design Justification**: General Purpose v2 accounts cater for all subservices including Blob, Files, Queue and Tables. The other accounts are for specialised requirements such as Azure Files with NFS, or block or page blobs. These can be used if required but will not be the default.

### Blob Tier Selection

**Design Reference:** Table 3 – [CO5](#_Storage_Account_and_1)

**Design Decision:** The default tier is Hot access. If the data to be stored is expected to be accessed fewer than every 90 days it should be placed in cool storage, and if it is expected to be accessed fewer than every 180 days it should be placed in the Archive tier.

**Design Justification:** The access tier chosen impacts the cost of the stored data. If the data is accessed frequently, it should be placed in the Hot tier to optimise costs. For anything that is less frequently accessed, between 90 days and 180 days estimate, it should be placed in the Cool tier. For anything that is for archival storage purposes or expected to be required less than every 180 days, the best cost configuration is to place this data in the Archive tier. This will need to be determined for each new storage account implementation requiring blob storage. However, as discussed in Section 5.3.12 an automation can be put in place to manage the lifecycle of blobs if the amount they will be accessed is unclear. In this case it is best to assume everything will be placed in the Hot tier, and the lifecycle policy will automatically move data into the appropriate tiers.

### Redundancy

**Design Reference:** N/A

**Design Decision:** The level of redundancy will be dependent on the Service Catalog tier. For Platinum, Gold, and Silver, the redundancy will be Geo-Redundant Storage (GRS), and Bronze will be Locally Redundant Storage (LRS) as the default.

**Design Justification:** Greater levels of redundancy also incur greater costs. As such the highest level of redundancy will be applied to the most critical workloads. Additionally, Australia Southeast as the Primary region has limitations in which redundancies can be applied. There are no Availability Zones as yet so Zone-Redundant and Geo-Zone Redundant options are unavailable. LRS will be used for Bronze workloads as this provides redundancy only within one data centre, but does not protect against a disaster. GRS will be used for Production, Platinum, Gold, and Silver workloads.

### Soft Delete

**Design Reference:** Table 2 – [R1](#_Storage_Account_and)

**Design Decision:** Soft-delete will be enabled for Blobs.

**Design Justification:** It is a security and reliability requirement to ensure that storage accounts with critical content in them are protected against accidental deletions and can be recovered in the case of a malicious attack.

**Design Details:** It is recommended that for Platinum applications or sensitive data the retention period is set to 30 days. For less critical systems this can between 7 and 14 days. For Gold and Silver a value of 14 days will be used. For Bronze and non-critical data 7 days will be used.

### Access and Authentication

**Design Reference:** [Table 2 – R2, R3](#_Storage_Account_and) and Microsoft Security Benchmark [IM-1](#_Overview)

**Design Decision:** Use Entra ID (previously Azure AD) for authentication. Local authentication should be disabled.

**Design Justification:** Using Entra ID for authentication prevents security issues and vulnerabilities that are associated with shared key access. Local authentication will not be enabled. If for any reason Azure AD cannot be used for a particular implementation the order of priority would be to use Shared Access Signatures (SAS) followed by Access Keys, although these are not preferred and will be disabled by default.

### Managed Identities

**Design Reference:** [Table 2 – R4](#_Storage_Account_and), Microsoft Security Benchmark [IM-3](#_Overview)

**Design** **Decision:** Managed Identities will be used to access Storage Account resources instead of Service Principals or other methods where possible.

**Design Justification:** Managed Identities are more secure and simpler to manage. Microsoft automatically rotates keys and secrets associated with Identities which removes the burden of secrets management when using Managed Identities for authentication. In this way credentials are not required to be stored anywhere and is entirely managed by Microsoft.

### Blob Versioning and Immutability

**Design Reference:** [Table 2 – R5](#_Storage_Account_and)

**Design Decision:** Blob versioning will be enabled if the select storage account type supports it.Though versions of Blobs are immutable, there is also an additional setting to set immutable storage on any Blob tier. Immutability will not be set by default as this will not allow users to modify or delete blobs and is cumbersome particularly during deployments. It is recommended to set immutability after a build is completed, and if the data is expected to be read-only and does not require constant modification.

**Design Justification:** Blob versions are immutable so the content of an existing blob version can’t be modified[[8]](#footnote-9). Note that having many versions of a blob can increase latency for blob operations, so Microsoft have recommended to maintain less than 1000 versions per blob, with a lifecycle management policy in place to delete old versions.

For immutability time-based retention and legal holds can be set. The minimum time-based retention is 24 hours, and the maximum is 400 years.

**Design Details:** The setting for blob versioning will be enabled by default on all storage accounts that support this feature.

### Network Access

**Design Reference:** [Table 2 – R6, R7, R8, R9](#_Storage_Account_and) and Microsoft Security Benchmark [NS-2](#_Overview)

**Design Decision:** Use Private Endpoint where feasible. Always ensure that public access is disabled. If Private Endpoint is not feasible for a given solution, ensure that the Firewall on the Storage Account is used to limit access to specific networks only. Additionally, allow access from trusted Microsoft resources.

**Design Justification:** Private Endpoint is the best option for the most secure connectivity, however having Private Endpoint for every resource in Azure can become cumbersome to manage. In cases where Private Endpoint is not used, access to the storage account from public will be disabled, and the local Firewall on the storage account will be used to whitelist only allowed networks for access. Note that when this is done, it will block access to Microsoft services as well that may need to interact with the Firewall. To avoid this issue, trusted Microsoft services will be allowed.

### Secure Transfer

**Design Reference:** [Table 2 – R10](#_Storage_Account_and)

**Design Decision:** Secure Transfer will be enabled.

**Design Justification:** Secure transfer ensures that all incoming requests must take place over HTTPS. Any requests that come through HTTP will fail which will maintain a healthy security posture.

### Shared Access Keys

**Design Reference:** [Table 2- R12, R13](#_Storage_Account_and), Microsoft Security Benchmark IM-8, DP-6

**Design Decision:** Shared Keys are the least preferred method of storage account access so should not be used by default.If shared keys are unavoidable a process must be in place to regenerate the keys periodically to avoid malicious attacks. As a default, this will be disabled.

**Design Justification:** Shared Keyscarry an innate risk of exposing data to malicious actors. As such it is best to avoid using them at all and instead use Azure AD authentication or Shared Access Signatures. If for some reason Shared Keys are unavoidable, an automation should be put in place to use a Managed Identity to automatically rotate the keys and place the new value in a Key Vault for the entities that require them to access the Storage Account. A similar process to what has already been defined in the Key Vault Core Service design will be used for this.

### SAS (Shared Access Signatures)

**Design Reference:** [Table 2 - R11, R14, R15](#_Storage_Account_and)

**Design Decision:** As with Access Keys, SAS will be disabled by default so that only Azure AD Authentication is allowed. If required this option can be overridden if approved for a particular deployment to allow Access Keys or SAS.

**Design Justification:** Access Keys and SAS tokens carry inherent risks and are the least preferred methods of authentication for Azure Storage Accounts. As such they will be disabled by default, and only enabled if approved for a particular deployment if there is no alternative.

If SAS tokens must be used, as they are the second most preferred method of authentication for Storage Accounts, they must be configured securely. This means they should only allow HTTPS connections, and a revocation plan must be in place to remove a SAS if it is compromised. Additionally, SAS tokens should only be in place for short-term expiration and only generated on an as-needs basis so that they are not available to be compromised.

### Blob Lifecycle Management

**Design Reference:** Table 3 – [CO2, CO3, CO5, CO6](#_Storage_Account_and_1)

**Design Decision:** A lifecycle policy will be created to automatically move data between storage tiers based on the frequency of access.

**Design Justification:** Leaving data in a suboptimal access tier often leads to unnecessary costs being incurred. It is difficult to monitor this manually, so the native solution of Lifecycle Policies will be used to automatically move data to a lower tier if it is infrequently accessed.

**Design Details:** The Lifecycle Policies should be set in accordance with the recommended level of access required to the data against each tier:

* Hot tier – frequently accessed data
* Cool tier – data less frequently accessed than every 30 days
* Archive tier – an offline tier for very infrequently accessed data, a minimum of 180 days

The lifecycle policies will be set to move data that has not been accessed for 30 days to the Cool tier, and data that has not been accessed for 90 days to the Archive tier.

### Data Protection

**Design Reference:** Microsoft Security Benchmark [DP-1](#_Overview)

**Design Decision:** Azure Purview integration with Azure Storage Account for data discovery and labelling is currently in Private Preview so will not be used[[9]](#footnote-10).

**Design Justification:** Services that are in the preview stage should generally not be used in production. Note that to meet this benchmark there is no current tooling configured to discover and label sensitive data. It is recommended to set-up and trial Azure Purview when it becomes Generally Available for Storage Account integration.

### Defender for Storage

**Design Reference:** Microsoft Security Benchmark [DP-2, LT-1](#_Overview)

**Design Decision:** Defender for Storage will be enabled.

**Design Justification:** Defender for Storage constantly analyses Blob and File services for malicious activity and generates alerts if anomalies are detected. In this way it supports Data Loss Prevention and enables thread detection capabilities. It will also make recommendations on more secure configurations for Storage Accounts.

### Data Encryption at Rest and In Transit

**Design Reference:** Microsoft Security Benchmark [DP-3, DP-4](#_Overview)

**Design Decision:** Data at Rest and In Transit encryption is enabled by default on Storage Accounts. The minimum TLS will be set to 1.2.

**Design Justification:** No action is required to enable encryption on Storage Accounts. The only setting required is to ensure a secure version of TLS is set as the minimum, which will be the recommended 1.2.

### Logging and Monitoring

**Design Reference:** Microsoft Security Benchmark LT-4

**Design Decision:** AllLogs and AllMetrics categories will be set for both the Storage Account and the Blob service.

**Design Justification:** The resource and audit settings are separate for the Storage Account and the blob service, but both will be configured to meet security requirements for diagnostics and audit logs.

### Backup

**Design Reference:** Microsoft Security Benchmark [BR-1](#_Overview)

**Design Decision:** Azure Backup will be enabled for Blobs.

**Design Justification:** To ensure that data is recoverable, backups will be enabled for blobs. Otherwise blobs that have been deleted beyond the soft delete point will not be recoverable.

**Design Details:** More specific details about the Backup Vault configurations will be provided in the Azure Backup Core Service design. For the Blob backup policies, there are two options for backups – Operational and Vaulted. The Vaulted option is currently in public preview so will not be used. It may be revisited when it becomes Generally Available. For the Operational backup option, the backup operation is performed continuously, and the following will be used for retention:

* Platinum – 30-day retention
* Gold and Silver – 14-day retention
* Bronze – 7-day retention

# Azure Policies

There are no additional Azure policies required.

# Configuration Templates

For storage accounts the baseline is assumed to be General Purpose v2 account type with Hot Access tier as the default as discussed in previous sections.

## Platinum Production

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| Subscription | AV ALZ [Subscription Name] |
| Name | saprdause[appname][workload]01 |
| Type | General Purpose V2 |
| Performance | Standard |
| Redundancy | RA-GRS |
| Secure Transfer | Enabled |
| Enable anonymous access on individual containers | Disabled |
| Enable storage account key access | Disabled |
| Default to Microsoft Entra authorisation in the Azure Portal | Enabled |
| Minimum TLS | 1.2 |
| Hierarchical Namespace | Disabled (can be enabled if required for a deployment) |
| Enable SFTP | Disabled (must enable Hierarchical Namespace if required) |
| Enable NFS v3 | Disabled (must enable Hierarchical Namespace if required) |
| Blob Access Tier | Hot |
| Networking | Private Access, Allow Trusted Microsoft Services |
| Network Routing | Microsoft Network Routing |
| **Lifecycle Management Policies** |  |
| Hot to Cool Rule | If blobs last modified more than 30-days ago, then move to cool storage |
| Cool to Archive Rule | If blobs last modified more than 90-days ago, then move to archive storage |
| **Backup Policy** |  |
| Name | blobplatinum-prd-ause-[appname]-[workload]-01 |
| Type | Operational |
| Retention | 30 days |
| **Data Protection** |  |
| Enable Soft-Delete for blobs | Enabled with 30-day retention |
| Enable Soft-Delete for containers | Enabled with 30-day retention |
| Enable Soft-Delete for files | Enabled with 30-day retention |
| Blob Versioning | Enabled |
| Backup | Enabled |
| **Diagnostics** |  |
| Storage Account Logs Captured | Transaction logs |
| Blob Logs Captured | allLogs and Transaction metrics |
| Log Analytics Workspace for logs | law-prd-ause-mgmt-01 |

## Platinum DR

Note that a storage account in the DR region may not specifically be required as the Production instance is set to Geo-Redundant Storage. However, if required by the application design, the following settings can be used:

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| Subscription | AV ALZ [Subscription Name] |
| Name | sadrauea[appname][workload]01 |
| Type | General Purpose V2 |
| Performance | Standard |
| Redundancy | LRS |
| Secure Transfer | Enabled |
| Enable anonymous access on individual containers | Disabled |
| Enable storage account key access | Disabled |
| Default to Microsoft Entra authorisation in the Azure Portal | Enabled |
| Minimum TLS | 1.2 |
| Hierarchical Namespace | Disabled (can be enabled if required for a deployment) |
| Enable SFTP | Disabled (must enable Hierarchical Namespace if required) |
| Enable NFS v3 | Disabled (must enable Hierarchical Namespace if required) |
| Blob Access Tier | Hot |
| Networking | Private Access, Allow Trusted Microsoft Services |
| Network Routing | Microsoft Network Routing |
| **Lifecycle Management Policies** |  |
| Hot to Cool Rule | If blobs last modified more than 30-days ago, then move to cool storage |
| Cool to Archive Rule | If blobs last modified more than 90-days ago, then move to archive storage |
| **Backup Policy** |  |
| Name | blobplatinum-dr-auea-[appname]-[workload]-01 |
| Type | Operational |
| Retention | 30 days |
| **Data Protection** |  |
| Enable Soft-Delete for blobs | Enabled with 30-day retention |
| Enable Soft-Delete for containers | Enabled with 30-day retention |
| Enable Soft-Delete for files | Enabled with 30-day retention |
| Blob Versioning | Enabled |
| Backup | Enabled |
| **Diagnostics** |  |
| Storage Account Logs Captured | Transaction logs |
| Blob Logs Captured | allLogs and Transaction metrics |
| Log Analytics Workspace for logs | law-prd-auea-mgmt-01 |

## Gold and Silver

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| Subscription | AV ALZ [Subscription Name] |
| Name | saprdause[appname][workload]01 |
| Type | General Purpose V2 |
| Performance | Standard |
| Redundancy | RA-GRS |
| Secure Transfer | Enabled |
| Enable anonymous access on individual containers | Disabled |
| Enable storage account key access | Disabled |
| Default to Microsoft Entra authorisation in the Azure Portal | Enabled |
| Minimum TLS | 1.2 |
| Hierarchical Namespace | Disabled (can be enabled if required for a deployment) |
| Enable SFTP | Disabled (must enable Hierarchical Namespace if required) |
| Enable NFS v3 | Disabled (must enable Hierarchical Namespace if required) |
| Blob Access Tier | Hot |
| Networking | Private Access, Allow Trusted Microsoft Services |
| Network Routing | Microsoft Network Routing |
| **Lifecycle Management Policies** |  |
| Hot to Cool Rule | If blobs last modified more than 30-days ago, then move to cool storage |
| Cool to Archive Rule | If blobs last modified more than 90-days ago, then move to archive storage |
| **Backup Policy** |  |
| Name | blobgoldsilverpolicy-prd-ause-[appname]-[workload]-01 |
| Type | Operational |
| Retention | 14 days |
| **Data Protection** |  |
| Enable Soft-Delete for blobs | Enabled with 14-day retention |
| Enable Soft-Delete for containers | Enabled with 14-day retention |
| Enable Soft-Delete for files | Enabled with 14-day retention |
| Blob Versioning | Enabled |
| Backup | Enabled |
| **Diagnostics** |  |
| Storage Account Logs Captured | Transaction logs |
| Blob Logs Captured | allLogs and Transaction metrics |
| Log Analytics Workspace for logs | law-prd-ause-mgmt-01 |

## Bronze Non-Production

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| Subscription | AV ALZ [Subscription Name] |
| Name | sa[env]ause[appname][workload]01 |
| Type | General Purpose V2 |
| Performance | Standard |
| Redundancy | LRS |
| Secure Transfer | Enabled |
| Enable anonymous access on individual containers | Disabled |
| Enable storage account key access | Disabled |
| Default to Microsoft Entra authorisation in the Azure Portal | Enabled |
| Minimum TLS | 1.2 |
| Hierarchical Namespace | Disabled (can be enabled if required for a deployment) |
| Enable SFTP | Disabled (must enable Hierarchical Namespace if required) |
| Enable NFS v3 | Disabled (must enable Hierarchical Namespace if required) |
| Blob Access Tier | Hot |
| Networking | Private Access, Allow Trusted Microsoft Services |
| Network Routing | Microsoft Network Routing |
| **Lifecycle Management Policies** |  |
| Hot to Cool Rule | If blobs last modified more than 30-days ago, then move to cool storage |
| Cool to Archive Rule | If blobs last modified more than 90-days ago, then move to archive storage |
| **Backup Policy** |  |
| Name | blobbronzepolicy-[env]-ause-[appname]-[workload]-01 |
| Type | Operational |
| Retention | 7 days |
| **Data Protection** |  |
| Enable Soft-Delete for blobs | Enabled with 7-day retention |
| Enable Soft-Delete for containers | Enabled with 7-day retention |
| Enable Soft-Delete for files | Enabled with 7-day retention |
| Blob Versioning | Enabled |
| Backup | Enabled |
| **Diagnostics** |  |
| Storage Account Logs Captured | Transaction logs |
| Blob Logs Captured | allLogs and Transaction metrics |
| Log Analytics Workspace for logs | law-prd-ause-mgmt-01 |

# Acceptance

Signature of this page by appropriately delegated representatives of ​Ambulance Victoria​ signifies acceptance of this design document.

Logicalis will commence build and implementation work once it receives a signed copy of this design document.

Signature of this page by appropriately delegated representatives of Ambulance Victoria signifies acceptance of this design document.

Logicalis will commence build and implementation work once it receives a signed copy of this design document.

|  |  |
| --- | --- |
| Project | Core Services |
| Document Version | 1.0 |

**Signed on behalf of Ambulance Victoria**

|  |  |
| --- | --- |
| Name | Dan Howarth |
| Position |  |
| Signature |  |
| Date signed |  |

**Signed on behalf of Logicalis Australia**

|  |  |
| --- | --- |
| Name | Daniela Nikolic |
| Position | Senior Cloud Engineer |
| Signature |  |

1. https://learn.microsoft.com/en-us/azure/well-architected/ [↑](#footnote-ref-2)
2. https://azure.microsoft.com/en-us/pricing/details/storage/blobs/ [↑](#footnote-ref-3)
3. https://learn.microsoft.com/en-us/azure/well-architected/resiliency/overview [↑](#footnote-ref-4)
4. https://learn.microsoft.com/en-us/azure/well-architected/cost/overview [↑](#footnote-ref-5)
5. https://learn.microsoft.com/en-us/azure/well-architected/scalability/overview [↑](#footnote-ref-6)
6. https://learn.microsoft.com/en-us/azure/well-architected/security/security-principles [↑](#footnote-ref-7)
7. https://learn.microsoft.com/en-us/azure/backup/blob-backup-overview [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/storage/blobs/versioning-overview [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline [↑](#footnote-ref-10)